REMARKS

Claims 5-11 stand rejected under 35 U.S.C. §102(b) as being anticipated by Tomko (US 5,790,668). This rejection is respectfully traversed on the following grounds.

Tomko pertains to a very robust method for controlling a database of confidential records such as medical records of information about a plurality of individuals. The method aims to protect the privacy of the enrolled individual owners of the database records from access by third parties and in certain embodiments, even from unauthorized administrators and operators of the database.

Applicant understands Tomko's disclosure as follows. An operator obtains from the enrollee information (a "profile") and encrypts the profile data with a random encryption key "K". The encrypted profile is stored as a database record at address "A" (col. 4, lines 23-26). The key K is then encrypted at least once with another random parameter "R" to generate one or more public keys P_{K1}, P_{K2} which are also stored at address A (col. 4, lines 26-37). The users of the information, i.e., so-called "authorized operators" have smart cards. When the authorized operators unlock private keys using their own fingerprints in connection with the smart cards, they are given access through a central processor to the public keys P_{K1} and P_{K2}. This enables the processor to extract the parameter R and encryption key K, and ultimately to decrypt the profile data (col. 4, line 52 to col. 5, line 52). This process of information transfer from the enrollee to the authorized user calls for the profile information to be encrypted once and decrypted once using an encryption key which is not based upon either the enrollee's fingerprint information or the authorized operator's fingerprint information.

The claimed invention is distinctly different from Tomko. According to claim 5, the information to be transmitted is encrypted with an encryption key based on a configuration derived from the first person-sender's fingerprint. The key encrypting the information is not randomly selected as in Tomko. Here, the encrypted information and the first key are given to the independent key control system. The control system decrypts the information with the first key and encrypts it a second time with a different encryption key. The second encryption key is based on a configuration derived from the second person-receiver's fingerprint. The newly encrypted information is transmitted to the recipient who can then decrypt it using the second encryption key which the recipient of course already possesses, having provided it to the control system.

It is seen that the fingerprints of both sender and receiver form the bases for the keys which encrypt/decrypt the information being sent. That is, the encryption keys are customized to the sender and receiver.

Not intending to disparage Tomko in any way but rather to point out distinctions, Applicant's invention has features that are advantageous in different information transfer circumstances from those of the reference. The claimed invention excels when transmitting a block of information between sender-receiver pairs. Each of the pair provides a customized key to the control system which decrypts the information supplied to it. The control system repackages the information in newly-encrypted form such that the ultimate intended recipient can access it.

In contrast, Tomko perhaps performs best in a situation where the recipients are authorized operators of the database system. They have been pre-screened and given smart cards encoded with private keys to access the database. Extraction of the private keys requires validation of the authorized operators' identities via fingerprint. The fingerprint essentially corroborates identity of the smart card holder in a way that allows the smart card to release a signal to the main processor to decrypt a database record for the authorized operator to access.

Similarly, the fingerprint of the enrollee in Tomko mainly serves to only uniquely identify the enrollee. When a person seeks to enroll in the system the processor checks whether or not the fingerprint already exists in the database already (col. 3, line 52 to col. 4, line 45). As a measure of security against access by unauthorized system operators, Tomko's method does not use the enrollee's fingerprint to encrypt the profile data. At col. 4, lines 46-49 Tomko recites:

> Thus, even if an unauthorized operator input a latent print to the biometric input device **20** seeking information on the individual bearing that fingerprint, no useful information would be retrieved.

Therefore, Tomko teaches away from Applicant's invention which does encrypt the transmitted information using a key derived from the sender's fingerprint.

Claims 6-11 incorporate the limitations of independent claim 5 and contain additional limitations. These claims are thus narrower than the independent claim and consequently are not anticipated by Tomko for the reasons discussed above.

For the foregoing reasons, Applicants respectfully request that the rejections be withdrawn and that claims 5-11 be allowed at this time.

Respectfully submitted,

Jeff C Lew

Date: June 2, 2005
2205 Silverside Road
Wilmington DE 19810
Facsimile:(302) 475-7915

Jeffrey C. Lew
Attorney for Applicant
Registration No. 35,935
Telephone:(302) 475-7919